Alexander A. Berengaut (*pro hac vice*)
Megan A. Crowley (*pro hac vice*)
COVINGTON & BURLING LLP
850 Tenth Street, NW
Washington, DC 20001
(202) 662-5367
aberengaut@cov.com
mcrowley@cov.com

Rob Cameron
Nathan D. Bilyeu
JACKSON, MURDO & GRANT, P.C.
203 North Ewing
Helena, MT 59601
(406) 389-8244
rcameron@jmgattorneys.com
nbilyeu@jmgattorneys.com

Attorneys for Consolidated Plaintiff TikTok Inc.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
MISSOULA DIVISION

SAMANTHA ALARIO, et al., *Plaintiffs*, and TIKTOK INC., *Consolidated Plaintiff*, v. AUSTIN KNUDSEN, *in his official capacity as Attorney General of the State of Montana*, *Defendant*.	CV 23-56-M-DWM CV 23-61-M-DWM **DECLARATION OF STEVEN WEBER**

I, Steven Weber, under penalty of perjury, hereby declare as follows:

1. I am a Professor of the Graduate School at the University of California, Berkeley, where I hold joint appointments as Professor at the School of Information and in the Department of Political Science. I am also the founder and former faculty director of the Center for Long Term Cybersecurity at UC Berkeley, where for seven years I led a multi-disciplinary research group that worked on emerging digital security issues at the confluence of new technologies, human behavior, and risk calculations made by firms and governments. In addition to my academic appointments, I am a Partner at Breakwater Strategy, a strategic insights and communications firm, where I assist clients with strategic decision-making and communications in areas that involve the intersection of technology and public policy. I received a Ph.D. in political science from Stanford University in 1989 and have been a professor at Berkeley since 1989. I have attached a true and correct copy of my curriculum vitae to this declaration.

2. My work focuses on U.S. national security issues with particular emphasis on how digital technologies impact and are impacted by national and international security. I have written three relevant university press peer-reviewed books and a number of peer-reviewed journal articles on this subject, as well as many other articles published in non-peer reviewed publications. I have served as a consultant to a wide variety of U.S. and global firms as well as U.S. government

agencies dealing with strategic issues at the intersection of national security and the digital economy.

3. I have been retained by the Consolidated Plaintiff TikTok Inc. in this action to analyze certain stated justifications for "An Act Banning TikTok in Montana" (the "Act"), which was signed into law by Governor Greg Gianforte on May 17, 2023. As I discuss below in greater detail, these justifications focus on three issues: (1) the security of the data that TikTok collects from its U.S. users, particularly as it relates to alleged disclosure to the Chinese government; (2) the possibility that TikTok's recommendation algorithm (*i.e.*, the computer code that selects what videos to present in a user's feed) could be misused for the benefit of the Chinese government, either by censoring certain content or promoting propaganda or disinformation; and (3) TikTok's alleged promotion of (or failure to remove) content that encourages minors to engage in dangerous activities, such as driving dangerously or taking excessive amount of medication.

4. As I discuss below, these issues are not unique or even distinctive to TikTok. (By TikTok, I mean to refer to the platform as opposed to any particular corporate entity.) It is inherent in digital technologies that every company, governmental entity, or non-governmental organization faces risks to the security

of the data that it stores—whether on behalf of employees, customers, or others.[1] Major companies such as Yahoo, LinkedIn, Meta, Marriott, Experian, Adobe, and many others have suffered well-known data breaches of millions of user records.[2] Likewise, with respect to the asserted issues pertaining to TikTok's algorithm, those are issues that social media and entertainment platforms (among many other industries) are dealing with more generally and have been for years. For example, YouTube has previously added disclaimers to certain channels that were reportedly being used to spread disinformation on behalf of the Russian government.[3] Similarly, Meta has announced that it has removed pages, groups, and accounts originating in Russia that engaged in coordinated inauthentic behavior.[4] Finally, every social media company and online entertainment platform that hosts user-

---

[1] *See, e.g.*, *Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts*, U.S. Dep't of Homeland Security (May 15, 2018), https://www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts.

[2] Michael Hill & Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO Online (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[3] Paresh Dave & Christopher Bing, *Russian Disinformation on YouTube Draws Ads, Lacks Warning Labels: Researchers*, Reuters (June 7, 2019), https://www.reuters.com/article/us-alphabet-google-youtube-russia/russian-disinformation-on-youtube-draws-ads-lacks-warning-labels-researchers-idUSKCN1T80JP.

[4] Nathaniel Gleicher, *Removing Coordinated Inauthentic Behavior from Russia*, Meta (Jan. 17, 2019), https://about.fb.com/news/2019/01/removing-cib-from-russia/.

generated content has had to contend with how to identify, evaluate, and remove potentially dangerous content. For example, YouTube has policies intended to address videos posted on that platform that involve "dangerous or threatening pranks" and "extremely dangerous challenges."[5]

5. Before turning to these specific issues, there are two general information security principles that should be kept in mind. First, data security is not a binary switch that can be toggled on or off. There are always tradeoffs being made among three components of security: confidentiality, integrity, and availability of data.[6] As with many enterprise risks, data security is an exercise in risk management—identifying risks, assessing them, and mitigating those risks to acceptable levels.[7]

6. Second, when it comes to data security threats, it is virtually impossible to prove the negative and establish that there are *no* risks to a particular

---

[5] *Harmful or Dangerous Content Policies*, YouTube, https://support.google.com/youtube/answer/2801964?hl=en (last accessed July 3, 2023).

[6] This "CIA" triad is carefully explained by the National Institute of Standards and Technology in *Standards for Security Categorization of Federal Information and Information Systems*, Fed. Info. Processing Standards Publication 199 (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[7] *Cybersecurity Strategy*, U.S. Dep't of Homeland Security (May 15, 2018), https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf; Nat'l Inst. of Standards & Tech., *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, at 13 (April 2013).

network or data storage and management system.[8] Sophisticated organizations and information security professionals understand that malicious actors and technology are constantly evolving, which means the threat landscape is always changing. Even an organization with strong security practices across the board cannot with full confidence assert that there is no risk that its data could be inadvertently accessed, improperly accessed, or disclosed. These principles form the basis of sophisticated data security programs and strategies in advanced organizations.

7. With the foregoing as background, I address the three issues cited as justifications for the Act: data security, the susceptibility of TikTok's algorithm to outside influence, and harmful content for minors.

I. Data Security

8. The first stated basis for the Act is that: "TikTok gathers significant information from its users" and "access[es] data against their will to share with the People's Republic of China." The Act further claims that "TikTok's stealing of information and data from users and its ability to share that data with the Chinese Communist Party unacceptably infringes on Montana's right to privacy" and that "TikTok's continued operation in Montana serves as a valuable tool to the People's Republic of China to conduct corporate and international espionage."

[8] Shuman Ghosemajumder, *You Can't Secure 100% of Your Data 100% of the Time*, Harv. Bus. Rev. (Dec. 4, 2017), http://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time.

9. As an initial matter, the assertion that TikTok "gathers significant information from its users" is principally a statement about data privacy, not data security. There is a separate policy debate about the extent to which social media and other digital product companies collect information from users, and this debate is beyond the scope of my testimony. The assertion that TikTok "access[es] data against [users'] will to share with the People's Republic of China," however, *is* an assertion about data security because it is an issue of who has access to data and for what purpose. I focus on principles of data security in analyzing this asserted basis for the Act.

10. To begin, I am unaware of any evidence—and the Act cites to none—suggesting that TikTok "access[es] data against [users'] will." To the contrary, as a condition of signing up for the app, users must agree to TikTok's Terms of Service, which, in turn, incorporate TikTok's Privacy Policy, which specifies the data that TikTok "may collect" from users, including "information that [they] provide, information from other sources, and automatically collected information."[9] It is common for social media platforms and other applications to collect this type of data from users, and it is equally common for users to agree to

[9] *Terms of Service*, TikTok (last updated May 2023), https://www.tiktok.com/legal/page/us/terms-of-service/en; *Privacy Policy*, TikTok (last updated May 22, 2023), https://www.tiktok.com/legal/page/us/privacy-policy/en.

this type of data collection pursuant to applications' terms of service.[10] Based on my review of TikTok's Privacy Policy, I understand users to authorize TikTok's collection of certain data, and thus I have no reason to believe that TikTok is "accessing data against [users'] will."

11. Notwithstanding the absence of evidence that TikTok "steal[s]" users' data, the Act expresses concern that TikTok "shares" user data—even if consensually obtained—"with the People's Republic of China." Again, this is a concern about third parties' access to data, the validity of which can be analyzed based on principles of data security.

12. As a threshold matter, in considering the national security concerns related to TikTok's user data, it is important to keep in mind the type of data we are discussing. As a recent report by the Internet Governance Project ("IGP") at the Georgia Institute of Technology explained, "[f]ull access to all TikTok data would provide [an actor with] aggregate data about the user population's video uploading and consumption behavior."[11] As the report explained, while such

[10] Milton L. Mueller & Karim Farhat, *TikTok and U.S. National Security*, Georgia Inst. of Tech. Internet Governance Project, at 19 (Jan. 8, 2023), https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf (explaining that "TikTok's behavior is not suspicious and it is not exfiltrating unusual data" and that "[w]hile TikTok collect[s] many data items, overall they still fall within general industry norms for user data collection").

[11] *Id.* at 20.

information may be "commercially valuable" to TikTok as well as certain developers and advertisers, it is unlikely to be particularly valuable to a foreign state like China, as it provides no "special insight into the control of critical infrastructure, military secrets, opportunities for corporate espionage, or knowledge of weapons systems."[12]

13. Even assuming some national security-related intelligence value for high-value targets (*e.g.*, individuals of particular interest from an intelligence perspective) could be derived from collecting a data set of commercially-focused information, the notion that the Chinese government would seek to amass this information by appropriating TikTok user data is not plausible, given the alternative means available to a nation state interested in acquiring information about individuals in another country. Those alternatives include purchasing information from data brokers (a practice in which U.S. intelligence agencies also engage), conducting open source intelligence gathering, and hacking operations like China's reported hack of the U.S. Office of Personnel Management ("OPM").[13] As such, it is relatively unlikely that a nation state actor, like China,

---

[12] *Id.*

[13] Byron Tau, *U.S. Spy Agencies Buy Vast Quantities of Americans' Personal Data, U.S. Says*, Wall St. J. (June 12, 2023), https://www.wsj.com/articles/u-s-spy-agencies-buy-vast-quantities-of-americans-personal-data-report-says-f47ec3ad; Josh Fruhlinger, Ax Sharma & John Breeden, *15 Top Open-Source Intelligence Tools*, CSO Online (June 28, 2021), https://www.csoonline.com/article/3445357/what-is-osint-top-open-source-

would rely on TikTok user data for intelligence-gathering purposes, given the existence of more effective and efficient means of obtaining relevant information about high-value targets.

14. I have reviewed publicly available information on Project Texas, TikTok Inc.'s initiative to safeguard U.S. user data and prevent foreign access to TikTok's data systems. These materials reflect a robust system of controls to mitigate data security risks that might arise were foreign governments to attempt to access protected U.S. user data.

15. For example, TikTok Inc. has formed a special-purpose subsidiary, TikTok U.S. Data Security Inc. ("USDS"), to oversee U.S. data systems, ensuring that protected U.S. user data will be under the control of a U.S.-led security team.[14] TikTok Inc. has also partnered with Oracle Corporation ("Oracle"), a prominent U.S. provider of FedRAMP- and DISA-compliant cloud-based applications and services. Currently, 100% of U.S. user traffic is routed to the Oracle cloud and

---

intelligence-tools.html; Josh Fruhlinger, *The OPM Hack Explained: Bad Security Practices Meet China's Captain America*, CSO Online (Feb. 12, 2020), https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

[14] Shou Chew, *Written Statement of Testimony*, U.S. House Comm. on Energy & Commerce, at 8 (Mar. 23, 2023), https://docs.house.gov/meetings/IF/IF00/20230323/115519/HHRG-118-IF00-Wstate-ChewS-20230323.pdf; *see also About Project Texas*, TikTok, https://usds.tiktok.com/usds-about/ (last accessed July 3, 2023); *Myths vs. Facts*, TikTok, https://usds.tiktok.com/usds-myths-vs-facts/ (last accessed July 3, 2023).

USDS infrastructure in the United States. In addition, TikTok Inc. reports that Oracle has begun reviewing TikTok's source code.

16. I am not aware of any other major social media or entertainment platform that maintains data security controls of the kind that have been announced regarding Project Texas.[15]

17. Finally, the Act expresses a concern about the ability of the Chinese government to use TikTok "to track the real-time locations" of certain individuals, including "public officials" and "journalists." This concern appears to be based on press reports that a few ByteDance employees used their previous access to certain TikTok user data to attempt to determine whether certain U.S.-based journalists were meeting with TikTok personnel.[16] As with the other data security issues

[15] Zoom Video Communications ("Zoom"), for example, has adopted some—but not all—of the protocols contemplated by Project Texas. Zoom has created a separate product—Zoom for Government—that includes security features beyond those included in Zoom's standard product and processes communications "exclusively in continental U.S. data centers that are managed solely by U.S.-based, U.S. people." Josh Rogin, *The White House Use of Zoom for Meetings Raises China-Related Security Concerns*, Wash. Post (Mar. 3, 2021), https://www.washingtonpost.com/opinions/2021/03/03/white-house-zoom-biden-meetings-china-cybersecurity/. TikTok, by contrast, has restructured the company to maintain a version of the TikTok platform for the U.S. in a U.S. subsidiary; erected software barriers to isolate the U.S. version of the TikTok app within the Oracle cloud; and granted Oracle—a U.S. company—access to its underlying source code.

[16] Emily Baker-White, *Lawmakers Express Outrage that TikTok Spied on Journalists*, Forbes (Dec. 23, 2022), https://www.forbes.com/sites/emilybaker-white/2022/12/23/lawmakers-outrage-tiktok-spied-on-journalists/; Emily Baker-White, *TikTok Spied on Forbes Journalists*, Forbes (Dec. 22, 2022),

discussed above, the data security concerns raised by this episode relate to an industry-wide issue: the potential access to, and misuse of, data by corporate insiders for purposes not authorized by company policy. For example, Google has reportedly terminated dozens of employees between 2018 and 2020 for abusing their access to the company's tools or data, including with respect to accessing Google user data.[17] As another example, in November 2022, Meta reportedly fired or disciplined more than two dozen employees and contractors who inappropriately took control of Facebook user accounts.[18] And Uber has settled claims related to the company's "God View" tool, which reportedly allowed employees to track the location of Uber riders without obtaining their permission.[19] Indeed, even outside

---

https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=e57a7a67da57; Mitchell Clark & Alex Heath, *TikTok's Parent Company Accessed the Data of US Journalists*, The Verge (Dec. 22, 2022), https://www.theverge.com/2022/12/22/23522808/tiktok-journalists-data-accessed-bytedance-internal-audit.

[17] Joseph Cox, *Leaked Document Says Google Fired Dozens of Employees for Data Misuse*, Vice (Aug. 4, 2021), https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse.

[18] Rohan Goswami, *Meta Reportedly Disciplined or Fired More than Two Dozen Workers for Taking Over Facebook User Accounts*, CNBC (Nov. 17, 2022), https://www.cnbc.com/2022/11/17/meta-disciplined-or-fired-employees-for-taking-over-user-accounts-wsj.html.

[19] Chris Welch, *Uber Will Pay $20,000 Fine in Settlement Over 'God View' Tracking*, The Verge (Jan. 6, 2016), https://www.theverge.com/2016/1/6/10726004/uber-god-mode-settlement-fine; Brian Fung, *Uber Settles with FTC Over 'God View' and Some Other Privacy Issues*, L.A. Times (Aug. 15, 2017),

the technology industry, the potential misuse of customer data by corporate insiders is a compliance challenge for virtually all companies.[20]

18. Because this risk is endemic to many industries, including the tech industry, in assessing the national security concerns associated with tech employees' access to user data, it is less important to consider the *presence* of the risk than it is to consider companies' *response* to the risk, including in particular how the company responds to specific instances of employee misconduct. In the case of TikTok, it has been reported that the company investigated the misconduct, disclosed its findings, took action against the employees involved, and implemented remediation efforts, including a restructuring of the department in which the employees involved in the misconduct were employed and reforms meant to strengthen the company's internal controls.[21] This response is indicative

---

https://www.latimes.com/business/technology/la-fi-tn-uber-ftc-20170815-story.html.

[20] *Credit Suisse Staffer Took Salary Data*, Reuters (Feb. 13, 2023), https://www.reuters.com/business/finance/credit-suisse-staffer-took-salary-data-bloomberg-news-2023-02-14/ (reporting that former Credit Suisse staffer misappropriated employee salary data as well as bank account information, Social Security numbers, and addresses); *Supermarket Morrisons Sued by Staff Over Personal Data Leak*, BBC News (Oct. 9, 2017), https://www.bbc.com/news/uk-england-41552911 (reporting that former grocery store employee misappropriated employees' personal data).

[21] David Shepardson, *ByteDance Finds Employees Obtained TikTok User Data of Two Journalists*, Reuters (Dec. 22, 2022), https://www.reuters.com/technology/bytedance-finds-employees-obtained-tiktok-user-data-two-us-journalists-2022-12-22/.

of a company making a good-faith effort to contend with an industry-wide compliance challenge, not a unique and extraordinary national security threat necessitating an outright ban of the platform involved.

II. Susceptibility of TikTok's Algorithmic Recommendation System to Outside Influence

19. The second stated justification for the Act pertains to TikTok's algorithmic recommendation system. Although not expressly stated in the Act, several legislators expressed concerns during official hearings that TikTok promotes propaganda on behalf of the Chinese Communist Party and/or that TikTok may be used for disinformation campaigns that benefit the Chinese Communist Party. For example, Representative Neil Duram asked a witness during a hearing whether the witness would "agree with [him] that TikTok is the music played by the Pied Piper to steal this generation's heart and mind?"[22] By this question, I understand Representative Duram to be asking whether a foreign actor could use TikTok to influence users' allegiances or belief systems by promoting and/or censoring certain content.

20. Witnesses at hearings on the TikTok Ban made this argument explicitly. For example, Bryan Burack of the Heritage Foundation suggested at a

[22] David McCabe, *A Plan to Ban TikTok in Montana Is a Preview for the Rest of the Country*, N.Y. Times (Apr. 12, 2023), https://www.nytimes.com/2023/04/12/technology/tiktok-ban-montana.html.

hearing of the Montana House Judiciary Committee that "[u]nder the control of the CCP, TikTok is the perfect tool for . . . political interference and influence operations."[23] And Keith Krach of the Krach Institute for Tech Diplomacy stated at the same hearing that TikTok is "a powerful propaganda tool."[24]

21. Before assessing these specific allegations, it is important to be clear about the applicable terminology. Specifically, it is important to draw a threshold distinction between "censorship" and "content moderation." The two concepts are not the same. The issue around censorship is whether an algorithm of this kind can be used to manipulate opinions or change perspectives in illegitimate ways; "content moderation," by contrast, refers to the legitimate removal or restriction of content that violates' platforms stated policies. Here again, content moderation is an industry-wide issue and not an issue limited to TikTok. Twitter attempts to block violence-promoting tweets.[25] Meta has an evolving set of policies that attempt to block various kinds of hate speech.[26] YouTube has modified its content promotion policies in an attempt to reduce radicalization, and in fact, the company

[23] Hearing on S.B. 419 Before the H. Comm. on Judiciary, 68th Leg., 2023 Sess. 8:18 (Mont. 2023).

[24] *Id.* at 8:20.

[25] *Twitter Rules*, Twitter, http://help.twitter.com/en/rules-and-policies/twitter-rules (last accessed July 3, 2023).

[26] *Community Standards*, Facebook, https://www.facebook.com/communitystandards/ (last accessed July 3, 2023).

reports that it removed over 5.6 million videos from the site in the 3-month period spanning October to December 2022.[27]

22. From a national security perspective, the question is whether the algorithm is legitimately shaping the flow of content in accordance with a commercial product strategy, along with appropriate restrictions to counter illegal or otherwise proscribed activity (such as hate speech) consistent with its public Terms of Service; or whether the algorithm is illegitimately seeking to manipulate perspectives and opinions in directions that serve a foreign state's short- and long-term strategic interests, which may be at odds with those of the United States.

23. Specifically with regard to TikTok, the question can be stated as follows: Is there evidence and reason to believe that TikTok is now or would become essentially an algorithmic propaganda tool of the Chinese government or the Chinese Communist Party? Based on the information that I have reviewed, my answer to this question is "no."

24. As an initial matter, a small number of anecdotes about allegedly "censored" or "promoted" content do not in and of themselves demonstrate a national security risk. That is partly because algorithmic content moderation and user experience customization is based on a fast-evolving science that involves

[27] *YouTube Community Guidelines Enforcement*, YouTube, https://transparencyreport.google.com/youtube-policy/removals?hl=en (last accessed July 3, 2023).

state-of-the-art machine learning techniques to solve some of the hardest problems in content recognition, natural language processing, and other technology that sometimes go under the label of "artificial intelligence." Like humans, algorithms can make mistakes and then learn from those mistakes (thus the term "machine learning" is a more accurate and useful descriptor than "artificial intelligence"). In most companies, algorithmic moderation is supplemented by human content moderators who typically make assessments about "gray" or uncertain cases where algorithmic decision-making is ambiguous or inconsistent, as well as overseeing how algorithms perform relative to the platforms' policies. The question, accordingly, is whether social media platforms react and evolve as they develop their technologies and practices over time and in response to concerns, complaints, and errors.

25. TikTok Inc.'s commitments through its Project Texas initiative indicate that it is responding to concerns about content moderation and evolving to address such concerns. For example, the materials that TikTok Inc. has publicly released on Project Texas reflect ongoing efforts by the company to address concerns about potential foreign state influence over TikTok's content, which TikTok is addressing in multiple ways.[28] For example, TikTok Inc. has contracted with Oracle, a U.S. company, to host the TikTok U.S. platform, and USDS runs

[28] Chew, *supra* n.14, at 7.

TikTok's recommendation algorithm for U.S. users in the Oracle cloud. TikTok Inc. has also engaged Oracle to review its content moderation system and algorithmic recommendation system to confirm that these systems operate in accordance with their design specifications, not some alternative set of principles or logic that might reflect foreign influence.

26. Recent academic studies further indicate that TikTok is honoring its commitment to responsible and viewpoint-neutral content moderation practices, notwithstanding certain anecdotal press reports to the contrary. For example, a 2022 report from the IGP, referenced above, found that videos depicting "content . . . known to be major Communist Party taboos," including "[s]upport for Hong Kong democracy protesters," were "easily . . . found on TikTok,"[29] rebutting earlier press reports that such videos were uncommon on TikTok.[30] The IGP report also found that searches related to the Chinese government's treatment of the Uyghur minority, an ethnic minority group based in China's Xinjiang Province, produced a list of search terms and videos "that by themselves are likely illegal on

[29] Mueller & Farhat, *supra* n.10, at 13.

[30] Drew Harwell & Tony Romm, *Inside TikTok: A Culture Clash Where U.S. Views about Censorship Often Were Overridden by the Chinese Bosses*, Wash. Post (Nov. 5. 2019), https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

Chinese social media."[31] Such evidence indicates that TikTok is neither promoting pro-China content nor censoring content that may be critical of China in a systematic way that supports allegations of a propaganda or disinformation campaign.

27. Based on these policies, practices, and evidence, it is my opinion that TikTok is not any more susceptible to foreign influence over its content than any other social media platform. On the contrary, as noted above, it is my opinion that TikTok Inc.'s Project Texas initiative sets standards for transparency and oversight that exceeds what is common in the industry.

III. Content Depicting Dangerous Activities

28. Finally, the Act purports to ban TikTok because it supposedly "fails to remove, and may even promote, dangerous content that directs minors to engage in dangerous activities." As explained above, this is an issue that affects every social media and entertainment platform that hosts user-generated content, and accusations of promoting dangerous content have been leveled at numerous platforms.[32]

29. Given the industry-wide challenge of harmful online content on the internet, the debate over whether TikTok poses a public safety threat comes down

[31] Mueller & Farhat, *supra* n.10, at 13.

[32] Adi Robertson, *Anti-Social Media Lawsuits Are Coming for Roblox and Discord*, The Verge (Oct. 6, 2022),

to the following question: Is there evidence or reason to believe that TikTok is purposefully promoting dangerous content on its platform or will prove unwilling or unable to remove such content posted by users? Here again, the available evidence indicates that the answer is "no." TikTok is plainly attuned to the issue of dangerous content on its platform and has taken multiple steps to address the issue, including by developing a set of Community Guidelines that govern the content that can be posted to the app; enforcing those Guidelines by removing violating content, often before such content receives any views; and creating unique experiences for teenage users that limit the type and amount of content they can view on the app.[33] Having reviewed TikTok's policies that limit access for

---

https://www.theverge.com/2022/10/6/23390796/roblox-discord-facebook-snapchat-social-media-lawsuits-addiction-child-abuse; Brandy Zadrozny, *'Carol's Journey': What Facebook Knew about How It Radicalized Users*, NBCNews (Oct. 22, 2021), http://www.nbcnews.com/tech/tech-news/facebook-how-radicalized-users-rcna3581; Donie O'Sullivan, Clare Duffy & Sarah Jorgensen, *Instagram Promoted Pages Glorifying Eating Disorders to Teen Accounts*, CNN (Oct. 4, 2021), https://www.cnn.com/2021/10/04/tech/instagram-facebook-eating-disorders/index.html.

[33] *Community Guidelines*, TikTok (last updated Mar. 2023), https://www.tiktok.com/community-guidelines/en/; *Community Guidelines Enforcement Report, January 1, 2023 – March 31, 2023*, TikTok (June 30, 2023), https://www.tiktok.com/transparency/en/community-guidelines-enforcement-2023-1/; *TikTok for Younger Users*, TikTok (Dec. 13, 2019), https://newsroom.tiktok.com/en-us/tiktok-for-younger-users; Cormac Keenan, *New Features for Teens and Families on TikTok* (Mar. 1, 2023), https://newsroom.tiktok.com/en-us/new-features-for-teens-and-families-on-tiktok-us.

younger users to certain types of content and/or provide parental controls for parents and guardians to do so and the policies of other major platforms, it is my view that TikTok's policies are at least as protective, and in some instances more protective, than other major platforms.

30. For example, TikTok has created a specific page about online challenges.[34] That page states that, although the majority of challenges on TikTok are "fun and safe," certain challenges may promote "harmful behaviors." The page therefore encourages users who encounter a challenge on the app to think critically about whether it involves "risky or harmful" behavior and, if so, to refrain from spreading the challenge and to report it in-app. These steps are not consistent with the assertion that TikTok promotes or fails to remove dangerous content.

IV. Conclusion

31. Social media and entertainment platforms, like TikTok, raise important policy issues, including the appropriate protection of user data, content moderation, and disinformation. These are legitimate issues to consider from a

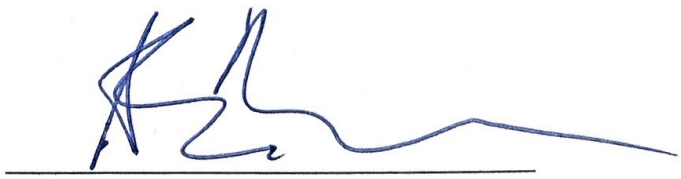
[34] *Online Challenges*, TikTok, https://www.tiktok.com/safety/en/online-challenges/ (last accessed July 3, 2023).

policy perspective, but they are issues that the industry confronts as a whole and are not unique or distinctive to TikTok.

32. As I have discussed above, TikTok's approach for dealing with these issues is in line with—and in many respects markedly better than—industry best practices, even for companies that hold significant sensitive user data. In light of the foregoing, there is no evident national security or public safety rationale for banning TikTok in Montana, as the Act has directed. It is arbitrary to select one market participant and ban that particular platform for policy issues that an entire industry faces. This is particularly the case where there exists alternative mechanisms—including the mitigation proposals that TikTok Inc. has outlined in connection with Project Texas—that enable the federal government to use regulatory frameworks like the Committee on Foreign Investment in the United States ("CFIUS") to mitigate security and safety risks around data and algorithms *beyond* what they would currently be able to achieve with peer firms.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 5th day of July, 2023.



Steven Weber